01 Jan 2007

Breaking the Cycle-Preventing Failures by Leveraging Historical Data During Conceptual Design

Daniel A. Krus

Katie Grantham
Missouri University of Science and Technology, kag@mst.edu

Breaking the Cycle – Preventing Failures by Leveraging Historical Data During Conceptual Design

Katie Grantham Lough* and Daniel Krus

Department of Interdisciplinary Engineering
University of Missouri-Rolla
Rolla, MO 65401

ABSTRACT

Major engineering accidents are often caused by seemingly minor failures propagating through complex systems. One example of this is an accident involving a Bell 206 Rotorcraft where a fuel pump failure led to the severing of the tail boom. Cataloguing and communicating the knowledge of potential failures and failure propagations is critical to prevent further accidents. The need for effective failure prevention tools is not specific to rotorcrafts, however. Failure reporting systems have been adopted by various industries to aid and promote failure prevention. The catalogued failures usually consist of narratives describing which part of a product failed, how it failed, and the circumstances behind the failure. While this information is vital to learning from past mistakes; often, the narratives are designed simply to report the events, not to use the data for product improvements or new designs. Therefore, more effective systems for cataloguing and utilizing corporate memory of recorded failure events are needed. This paper presents the design of a computational database to support the failure prevention tool, the function based failure propagation (FFP) method. FFP promotes failure prevention by identifying failure propagation paths through a system as early as the conceptual phase of product design, where impacts of failure prevention are greatest. It uses a database populated by historical failure information to present specific paths that potential failures might take as they propagate through a system. The information communicated by the FFP method is the potential location of and likelihood failure propagations.

1. INTRODUCTION

Major engineering accidents are often caused by seemingly minor failures propagating through complex systems. Two examples of this type of failure propagation are present in the National Transportation Safety Board (NTSB) accidents of the Bell 206 Rotorcraft. Accidents MIA86LA133[1] and DEN88LA180[2] experienced initial failures of a battery generator and a fuel pump, both of which led to the severing of the tail boom leaving the rotorcraft unusable and causing devastating injuries to its occupants. Cataloguing and communicating the knowledge of potential failures and failure propagations is critical to prevent further accidents. The need for effective failure prevention tools is not specific to rotorcrafts, however. Failure reporting systems have been adopted by various industries to aid and promote failure prevention. The catalogued failures usually consist of narratives describing which part of a product failed, how it failed, and the circumstances behind the failure. While this information is vital to learning from past mistakes; often, the narratives are designed simply to report the events, not to use the data for product improvements or new designs.

Probabilistic risk assessments (PRA) are used most often in design and manufacture to estimate the risk of product failure. The Risk in Early Design (RED) method is a PRA that enables risk assessment in conceptual product design by leveraging historical failure data. However, RED can only calculate risk based on single failures, not ones that propagate through a system, leaving the devastating effects of the above rotorcraft accidents unforeseen. Therefore, more effective systems for cataloguing and utilizing corporate memory of recorded failure events are needed. This paper presents the design of a computational database to support the failure prevention tool, the function based failure propagation (FFP) method.

* Corresponding author: Tel.: (573) 341-4598; Fax: (573) 341-6593; E-mail: kag@umr.edu

2. BACKGROUND

2.1. The Risk in Early Design (RED) Method

The risk in early design (RED) method is a PRA that collects failure data from historical events, and combines it with functional models to perform risk analysis as early as the conceptual phase of product design [3]. RED presents a listing of the likelihood and consequence of function-failure mode pairs plotted on a risk fever chart. Since the RED risks are automatically obtained from historical failure data, RED allows even novice engineers or those unfamiliar with the systems being analyzed to perform a detailed analysis on that system. RED can detect specific function-failure pairs during the conceptual design phase; however, each entry returned is regarded as a separate and singular case, not part of any other failure [4, 5]. Thus, this method does not consider combinations of failures or their sequence.

2.2. Event Tree Analysis

Event Tree Analysis is a PRA that uses forward logic to plot a path from an initial failure to its potential outcomes [6]. Starting with the initiating failure, termed an initiating event, paths called branches are created along other events that can occur after the initiating event, in approximately chronological order. Each of these events is limited to an outcome of success or failure, creating a number of unique branches made up of the successes and failures of the entire chain of events [7]. Unlike RED, Event Tree Analysis details the many different paths that can lead to the failure of a system. However, it requires expert solicitation to determine the initiating events or effect of those events, which may be subjective or not available. Finally, this analysis focuses on events occurring in a mature system, making it ill-suited for use during the conceptual product design.

2.3. Fault Tree Analysis

Fault Tree Analysis uses backwards logic to plot a path from an ultimate failure to each of its potential causes [8, 9]. Beginning with the ultimate failure or fault, potential causes of the failure are found and plotted, using Boolean gates such as “And” or “Or.” For each of these causes, more faults are identified, until the most basic causes of the top fault are found. Using the tree structure and the probabilities of each fault occurring, the probability of each branch of faults leading to the top fault is calculated, as well as the total probability of the top fault occurring [10]. Fault Tree Analysis, like Event Tree Analysis, focuses on chains of faults propagating in a system. Also, each fault tree created is specifically tailored to its top fault, focusing in on a particular fragment of the system rather than the system as a whole [8]. While Fault Tree Analysis does model chains of faults as they spread through a system, it too requires experts to brainstorm the faults and works best on a mature system, and is thus not suited for use in the conceptual design phase.

2.4. Function Failure Propagation

Function Failure Propagation is a method that uses historical failure propagation data to calculate the likelihood of a chain of failures occurring [11]. Using the flows in a functional model as “common interfaces” between functions, propagation trees that show all the paths that failures can propagate to a function are created. RED is used to identify the most likely functions to start chains of failures, and analysis determines the functions most important to the system. Using these most likely failures and most important functions as the starting and ending points of the analysis, the likelihood of each chain is calculated by using the collected historical failure propagation data and the Boolean operators “And” and “Or.” This returns a relative likelihood between zero and one. FFP hocuses on chains of function failures and how they propagate through a system. As it uses a functional model as its basis, it is well-suited for use in the early design. It relies on collected historical data to determine the likelihoods of those chains, removing much of the subjectivity of the analysis. However, it is extremely dependant on the data collected in it knowledge base, and returns poor or incorrect results if entries are not present in the knowledge base matrix. Thus, to properly utilize this method, a well-populated knowledge base must exist.

3. FAILURE PROPAGATION CATALOGUING PROCEDURE AND BELL 206 ROTORCRAFT FAILURE CATALOGUING EXAMPLE

In order to collect failure propagation data, reports or other records of failures must be analyzed. Each accident or failure report must be applied to a functional model in order to plot the path, if any, of the failure as it propagates through the system. Thus, for any data collection to take place, a functional model of at least the systems involved in the report must exist.

The reports used in this study are National Transportation Safety Board accident reports for Bell 206 helicopters. From an initial analysis of the reports, the systems that would be necessary to model were the fuel and air systems, the turbo shaft engine, the main and tail rotors, the lubrication system, the electrical system, the passenger compartment, and the controls and sensors. Once these systems are modeled and combined together to form a single system, data from the reports can be collected. The functional model of the Bell 206 helicopter used to collect the data from the NTSB reports is shown in Figure 1.

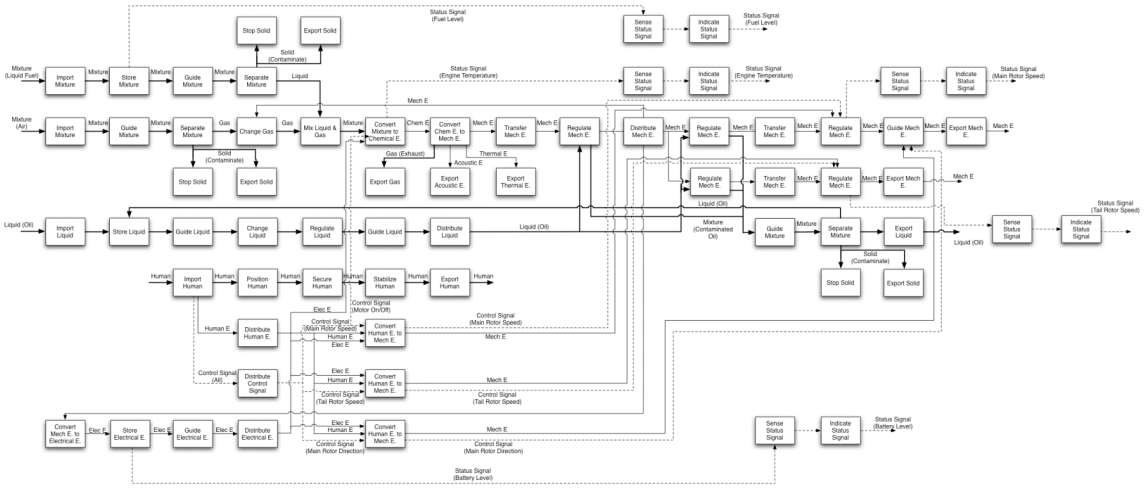

Figure 1. Bell 206 Helicopter Functional Model

Each report is then analyzed individually to find all the recorded failures. Each failure is recorded along with its failure mode and corresponding function or functions. As an example, in NTSB report MIA86IA250[12], an engine flameout is mentioned, as is fuel contamination and a blocked fuel filter. From these mentioned events, two failures were recorded. The engine flameout was due to lack of fuel, or "no flow," as mentioned in the report, and was a failure of the function "convert mixture to chemical energy." The blocked filter was a failure of the "separate mixture" function and was caused by contamination of the mixture with particles of unexpected size. The report also states that the helicopter crashed after the flameout, thus the main rotor, "export mechanical energy," also failed, due to lack of power. This example of collected data is shown in Table 1.

Table 1. Partial Listing of Collected Failure Data

Report: FTW85LA295 **Cause(s):**	**Failure Mode:**	**Corresponding Function:**
Tail rotor failure	Unknown	Regulate Mechanical energy
Hard landing	Rapid descent	regulate Mechanical Energy
Tail boom severed	Impact Fracture	Secure Solid, transmit ME, guide ME, etc…..
Report: LAX89LA297 **Cause(s):**	**Failure Mode:**	**Corresponding Function:**
Loss of engine power	Fuel contamination	Convert Chemical Energy to Mechanical Energy
Report: FTW89FA075 **Cause(s):**	**Failure Mode:**	**Corresponding Function:**
Blocked & Collapsed fuel nozzle screen	Overstress & contamination	Separate Mixture
Fuel filter cap bypass valve stuck open in bypass mode	Galling	regulate liquid
Bypass valve sensor light not working correctly (intermittent operation)	Unknown	Sense Status Signal
Loss of engine power	Fuel starvation	Convert Chemical Energy to Mechanical Energy
Report: MIA86IA250 **Cause(s):**	**Failure Mode:**	**Corresponding Function:**
Engine flameout	Fuel Starvation	Convert Chemical Energy to Mechanical Energy
Fuel Filter completely blocked	Contamination	Separate Mixture

Once these failures have been collected, they can then be plotted on the functional model of the system. These failures are placed on the functional model, and the path between them, from the first occurring failure to the final failure, is plotted. Continuing the above example, the filter became blocked, then the engine flameout occurred, and finally the main rotor lost power. Thus, failure propagates from "separate mixture" to "convert mixture to chemical energy" to "export mechanical energy" by way of other functions, as shown in Figure 2. The failure of the "separate mixture" causes the liquid-solid mixture flow to be stopped, and this "no flow" continues to propagate through "convert mixture to chemical energy" and to "export mechanical energy," stopping the chemical energy and mechanical energy flows. Finally, the other mechanical energy flow to the tail rotor would also be stopped, causing these functions to fail as well, even though not mentioned in the actual report.

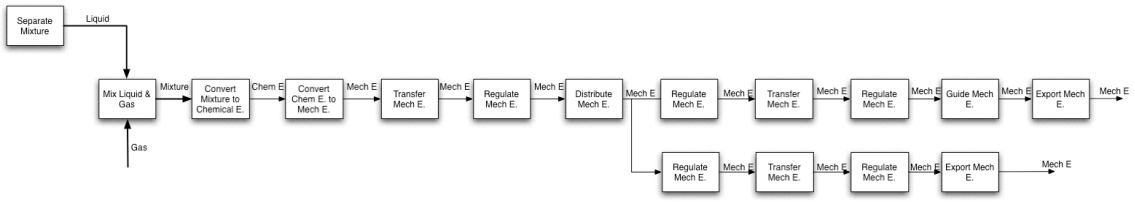

Figure 2. MIA86IA250 Failure Propagation Path

Once the propagation path has been found, the propagation data can then be tabulated. For this path, there are fifteen propagations to record. Each of these propagations increments its entry in the propagation knowledge base matrix, as shown in Figure 3. This is then repeated for other reports, further populating the knowledge base.

Initiating Function \ *Dependent Function*	Separate Mixture	Mix Liquid & Gas	Convert Mixture to Chemical Energy	Conver Chem E. to Mech E.	Transfer Mech E.	Regulate Mech E.	Distribute Mech E	Guide Mech E	Export Mech E
Separate Mixture		1							
Mix Liquid & Gas			1						
Convert Mixture to Chemical Energy				1					
Conver Chem E. to Mech E.					1				
Transfer Mech E.						3			
Regulate Mech E.					2		1	1	1
Distribute Mech E						2			
Guide Mech E									1
Export Mech E									

Figure 3. Propagation Knowledge Base Matrix with Data from MIA86IA250

Once the knowledge base has been populated, the data must be converted to likelihood values that can be used with the Boolean operators used in function-based failure propagation. The integer values contained in the knowledge base are then converted to decimal numbers between zero and one using Equation (1), to allow use with Boolean operators. In a M x M knowledge base matrix, $l_{i,j}$ is the likelihood of the i,j^{TH} pair, where I and j are the initiating and dependent functions, respectively. $n_{i,j}$ is the number of times the i,j^{TH} pair has occurred. A sample calculation of the likelihood of "regulate mechanical energy" to "transfer mechanical energy" is shown in Equation 2. The converted knowledge base for MIA86IA250 is shown in Figure 4.

$$l_{i,j} = \frac{n_{i,j}}{\max\limits_{\substack{1<i<M \\ 1<j<M}} (n_{i,j})} \tag{1}$$

$$l_{RME,TME} = \frac{n_{RME,TME}}{\max\limits_{\substack{1<i<M \\ 1<j<M}} (n_{i,j})} = \frac{2}{3} = .66 \tag{2}$$

Initiating Function	Separate Mixture	Mix Liquid & Gas	Convert Mixture to Chemical Energy	Conver Chem E. to Mech E.	Transfer Mech E.	Regulate Mech E.	Distribute Mech E	Guide Mech E	Export Mech E
Separate Mixture		0.33							
Mix Liquid & Gas			0.33						
Convert Mixture to Chemical Energy				0.33					
Conver Chem E. to Mech E.					0.33				
Transfer Mech E.						1.00			
Regulate Mech E.					0.67		0.33	0.33	0.33
Distribute Mech E						0.67			
Guide Mech E									0.33
Export Mech E									

Figure 4. Converted Knowledge Base for MIA86IA250

4. CONCLUSION

This paper presents the design of a computational database to support the failure prevention tool, the function based failure propagation (FFP) method. This database, combined with the FFP method, provides designers a method to anticipate how subsystem failures will affect the operation of the complex systems they are designing. This big picture view is obtainable during the conceptual phase of design since the failure propagation information is catalogued by function. Since the data is easily available so early in the design process it has the greatest chance of preventing devastating accidents such as the NTSB accidents of the Bell 206 Rotorcraft.

5. REFERENCES

1. Board, N.T.S., *Bell 206 Rotorcarft Accident*.
2. Board, N.T.S., *Bell 206 Rotorcraft Accident Report*.
3. Grantham Lough, K., *Risk in Early Design*. 2005, University of Missouri-Rolla.
4. Grantham Lough, K., R. Stone, and I. Tumer. *Prescribing and Implementing the Risk in Early Design (RED) Method*. in *Proceedings of DETC'06*. 2006. Philadelphia, PA.
5. Grantham Lough, K., R. Stone, and I. Tumer. *The Risk in Early Design (RED) Method: Likelihood and Consequence Formulations*. in *Proceedings of DETC'06*. 2006. Philadelphia, PA.
6. Frank, M.V. *Reentry safety: probability of fuel release*. in *ESREL '99*. 1999.
7. *Reactor Safety Study: An Assesment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix I: Accident Definition and Use of Event Trees*, U.S.N.R. Commission, Editor. 1975.
8. Vesely, W.E., et al., *Fault Tree Handbook*, U.S.N.R. Commision, Editor. 1981, U.S. Government Printing Office.
9. Kumamoto, H. and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*. 2nd ed, ed. J.B. Anderson. 1996, New York: IEEE Press.
10. Bedford, T. and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. 2001, Cambridge: Cambridge University Press.
11. Krus, D., and Grantham Lough, K., *Applying Function-Based Failure Porpagation Analysis in Conceptual Design*, in *American Society of Mechanical Engineers International Design Engineering Technical Conference*. 2007: Las Vegas, NV.

12. Board, N.T.S., *Bell 206 Rotorcraft Accident*.